United States Military Academy

West Point, New York 10996

Network-Centric System Implications for the Hypersonic Interceptor System

OPERATIONS RESEARCH CENTER OF EXCELLENCE
TECHNICAL REPORT DSE-TR-0547
DTIC #: ADA434078

Paul D. West, Ph.D.
Assistant Professor, Department of Systems Engineering

Approved by
Colonel Michael L. McGinnis, Ph.D.
Professor and Head, Department of Systems Engineering

May 2005

The Operations Research Center of Excellence in supported by the
Assistant secretary of the Army (Financial Management & Comptroller)

Network-Centric System Implications for the Hypersonic Interceptor System

OPERATIONS RESEARCH CENTER OF EXCELLENCE
TECHNICAL REPORT DSE-TR-0547
DTIC #: ADA434078

Paul D. West, Ph.D.
Assistant Professor, Department of Systems Engineering

Approved by
Colonel Michael L. McGinnis, Ph.D.
Professor and Head, Department of Systems Engineering

May 2005

The Operations Research Center of Excellence in supported by the Assistant Secretary of the Army (Financial Management & Comptroller)

Executive Summary

This report identifies the qualities and attributes of network-centric systems (NCS), describes a taxonomy of 13 critical NCS risk factors, and outlines a value-based model for NCS risk management, all as they affect the operation of a hypersonic interceptor (HSI) system.

Successful employment of an HSI system requires a thorough integration of operations into the larger NCS super-system. Required capabilities previously identified for an HSI indicate the intent for this system is to function in full collaboration with the Joint Exercise Support System Intelligence Module (JIM), Unit of Employment (UE), and Unit of Action (UA) forces, which will operate in a network-centric framework.

Based on these required capabilities and the common NCS factors, it is recommended that the Hypersonic Interceptor IPT identify specific measures of effectiveness (MOE) relevant for system risk management in an NCS environment and incorporate these measures and the methodology described in this report into the system life-cycle management plan.

Specific actions to implement these recommendations include the development of a decision support tool to assess key stakeholder risk profiles and to model attribute weights in pre- and ongoing HSI operations, development of MOE to assess ongoing and post-operations analysis, and collaboration with engineers and operators of related NCS node programs.

About the Author

Dr. Paul West is an Assistant Professor in the Department of Systems Engineering at the United States Military Academy at West Point. His research interests include the design and operation of network-centric systems, the representation of human behaviors in blended constructive, virtual, and live military operations, and information visualization. He received a BS from the State University of New York at Albany, an MBA from Long Island University, a Master of Technology Management from Stevens Institute of Technology, and an interdisciplinary Ph.D. in Systems Engineering and Technology Management, also from Stevens. He is a former Abrams tank Master Gunner with more than 14 years' military experience in Armor, Cavalry, and Headquarters, Department of the Army, assignments.

Acknowledgements

This report describes work conducted as part of the Department of Systems Engineering support for the Hypersonic Interceptor Integrated Project Team (HSI IPT). The overall DSE effort was directed by **Dr. Bobbie L. Foote**.

Table of Contents

List of Figures

List of Tables

List of Equations

Chapter 1. Overview of Network-Centric Systems

The dawning of the Information Age has fostered growth of network-centric systems (NCS) and strategies for capitalizing on their strengths in both the military and commercial arena. This report describes attributes of NCS and the environment in which they operate, with special consideration of hypersonic interceptor (HSI) systems.

Complex, functionally distributed organizations are increasingly harnessing powers of agility and self-synchronization to gain competitive advantage. Networks of "knowledgeable nodes" are emerging to compete for dominance over large – possibly global – regions. Capabilities previously confined to self-contained, single-function systems may be distributed worldwide and support multiple autonomous nodes.

Leveraging distributed capabilities in the information, cognitive, and physical domains requires architectures to move from a platform-centric to a network-centric structure. One example of a system making this transition is found in the U.S. Army's deployment of combat power via the Future Combat System (FCS). For a HSI system to play a key role in this distributed form of warfare, it must be seen and behave as a node in the larger network-centric system.

1.1. Domains of Network-Centric Systems

Following the successful business model bearing a similar name, "just-in-time warfare" [1] adapts peer-to-peer (P2P) network concepts to a broad range of military operations. These operations are grouped under the banner, "Network-Centric Warfare" (NCW), popularized by Alberts, Garstka and Stein in *Network Centric Warfare – Developing and Leveraging Information Superiority*. [2] In it, they say that battlespace entities have three primary functional modes: sensing, deciding, and acting, all within the context of shared situational awareness. The degree to which one functional mode dominates at a particular point in time, they say, determines the role of the entity in a military operation.

Stein [3] observes that information flow between nodes suggests that three sub-architectures exist:

- **Information grid**, providing the infrastructure to receive, process, transport, store, and protect information.

- **Sensor grid**, providing a high degree of awareness of friendly forces, enemy forces, and environment across the battlespace.

- **Shooter grid**, tasked to create necessary effects on the battlefield, then dynamically re-tasked as necessary.

These grids form a three-dimensional physical array with no prescribed pathways between nodes. Instead, nodes sharing a common relevant operating picture are able to choose "best" pathways in real-time, given the current states of all nodes in the network.

The domains in which nodes operate are described in the U.S. Department of Defense (DOD) *Report to Congress* on NCW [4] as the

- **Cognitive domain**, where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sense-making, decisions are made.

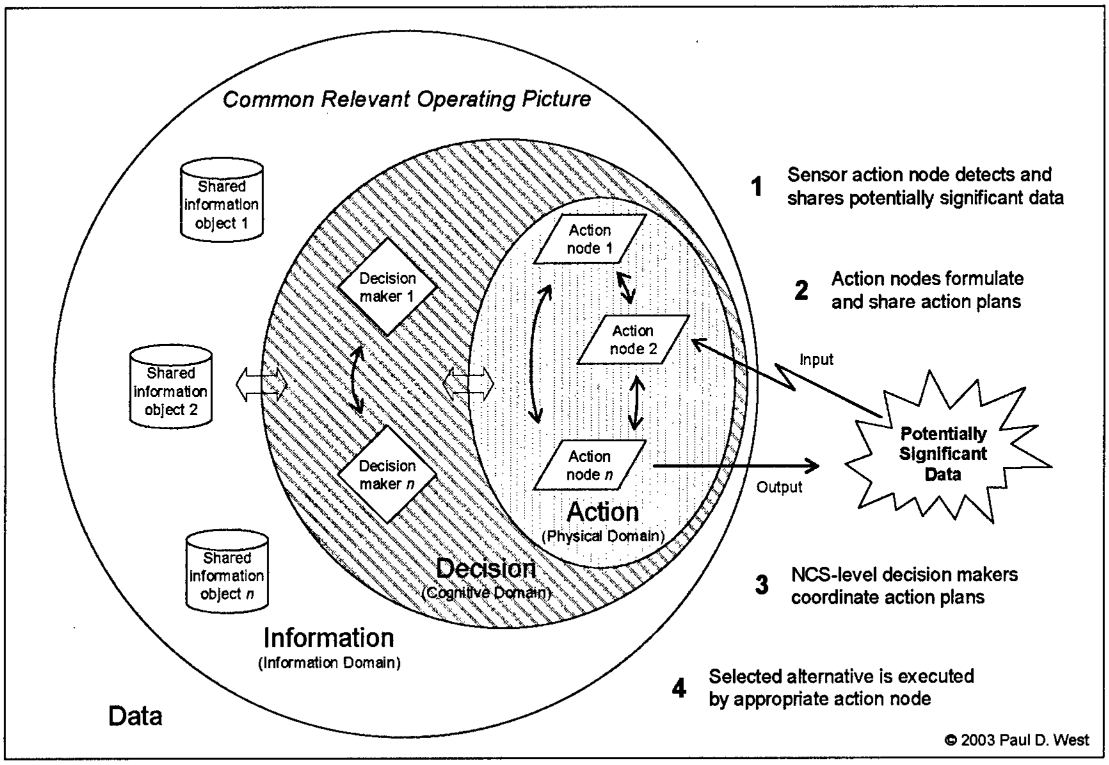
- **Information domain**, where information is created, processed and shared.

- **Physical domain**, where physical platforms and the communications networks that connect them reside.

These overlapping domains extend to a four-dimensional network of information, decision, and action nodes that share a common relevant operating picture (CROP). This enables nodes to self-synchronize and achieve desired effects with or without a central command and control facility. The fourth dimension, time, applies in that the CROP is constantly undergoing change as operations continue.

The Venn diagram in Figure 1 illustrates the relationships between domains. Nodes in all domains are capable of creating, processing and sharing information and are members of the information domain. Action nodes are also capable of some level of decision making and thereby co-exist in the cognitive domain. Situation awareness is shared across all domains and is available to all nodes.

The DOD report cautions against ascribing concepts such as "Sensor Grid" to any single domain. "Complicating [the formulation of a generally agreed taxonomy for NCW concepts] is the tendency for some concepts to be described strictly in the context of a single domain, when in reality, all three domains must often be employed to uniquely characterize a concept."



Common Relevant Operating Picture
Shared information object 1
Shared information object 2
Shared information object n
Decision maker 1
Decision maker n
Action node 1
Action node 2
Action node n
Action
(Physical Domain)
Decision
(Cognitive Domain)
Information
(Information Domain)
Data
1 Sensor action node detects and shares potentially significant data
2 Action nodes formulate and share action plans
Input
Output
Potentially Significant Data
3 NCS-level decision makers coordinate action plans
4 Selected alternative is executed by appropriate action node
© 2003 Paul D. West

Figure 1: Domains of Network-Centric Systems

1.2. Key Functions of Network-Centric Warfare

Network-centric warfare relies on rapid, accurate and timely information to fuel two major functions: speed of command and self-synchronization. Vice Admiral Arthur Cebrowski, while Director for Space, Information Warfare, Command and Control, in the office of Chief of Naval Operations, and John Garstka, Scientific and Technical Advisor for the Directorate for C4 Systems on the Defense Department's Joint Staff, defined these functions as follows [5]:

"*Speed of Command* is the process by which a superior information position is turned into a competitive advantage. It is characterized by the decisive altering of initial conditions, the development of high rates of change, and locking in success while locking out alternative enemy strategies. It recognizes all elements of the operating situation as parts of a complex adaptive ecosystem and achieves profound effect through the impact of closely coupled events."

"*Self-Synchronization* is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement. Self-synchronization is enabled by a high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment. It overcomes the loss of combat power inherent in top-down, command-directed synchronization characteristic of more conventional doctrine and converts combat from a step function to a high-speed continuum."

A network-centric combat system de-aggregates the battlefield functions found in a platform-centric system. Such a system must be amorphous, drawing upon the "best" mix of capabilities available to meet a specific requirement under specific conditions. A configuration also may change through time during a mission.

Critics of NCW suggest that its two main functions, speed of command and self-synchronization, may be its own worst enemy. The speed of command function is often discussed in terms of an *observe*, *orient*, *decide*, *act* cycle, or "OODA loop." [6] This characterization of the decision cycle, shown in Figure 2, has two main implications for NCW. First, if *A* can complete the cycle faster, it will maintain the initiative over *B*. Second, if *A* can act while *B* is still in the OO stages, it can engineer "observations" for *B* and thereby manipulate the remaining ODA stages. However, critics say, if *A*'s OODA loop is too short, its processing speed may force it to incorrectly assess *B*'s indecisiveness and falsely orient, decide and act on its own observation of *B*'s behavior. [7] This feature may have significant implications for a hypersonic interceptor, since its extreme speed enables controllers to completely shape the engagement window.

Similar dangers can be seen in self-synchronization. This process contains four key elements: [6]

- two or more robustly networked entities (nodes),

- a shared awareness,
- a rule set, and
- a value-adding interaction.

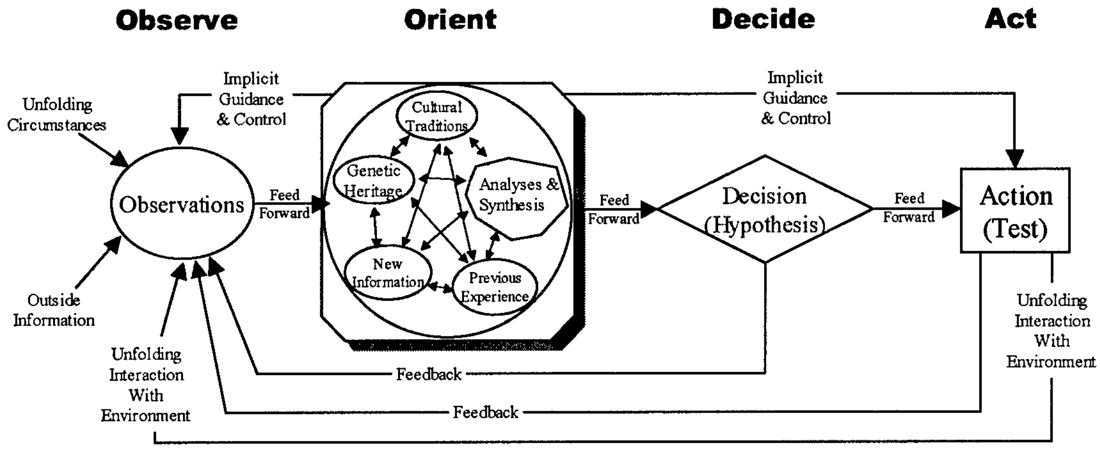


Figure 2: The OODA Loop [6]

Alberts, Garstka and Stein [2] point out that the combination of a rule set and shared awareness allows entities to operate separately from traditional mechanisms of command and control. The rule set further describes desired outcome for various situations. Given these objectives and goals, or "commander's intent," and a shared awareness of the situation, an NCW system should be able to synchronize itself from the bottom up. However, a shared *but inaccurate* awareness brought on by an accelerated OODA loop, catastrophic failure of a key networked node, or a failure of the information grid could result in failure of the system or its super or lateral systems.

Network-centric operations (NCO) have additional complexity in the Information Age due to the asymmetric nature of conflict afforded by availability of information and the ensuing shift from *event-based* operations to *effects-based* operations.

Attrition-based operations characteristic of symmetric conflict are now the exception rather than the norm. World Wars I and II, the Cold War and Desert Storm have given way to September 11th, Operation Enduring Freedom (OEF), and Operation Iraqi Freedom (OIF). In asymmetric conflict, competitors have unequal means and will, and psychological effects are often more significant than physical effects.

1.3. Effects Based Operations

Effects-based operations (EBO) are key to network-centric systems. They may be defined in the military realm as coordinated sets of actions directed at shaping the behavior of friends, neutrals and foes in peace, crisis, and war. [9] The U.S. Joint Forces Command defines it as, "A process for obtaining a desired strategic outcome or 'effect' on the enemy, through the synergistic, multiplicative, and cumulative application of the full range of military and nonmilitary capabilities at tactical, operational, and strategic levels." [10]

"If the enemy is a complex, adaptive system," said Dave Ozolek, Assistant Director, Joint Experimentation, U.S. Joint Forces Command, "then perhaps we can control his behavior by manipulating his environment, pre-empting his adaptive options." [8]

This behavior modification is achieved by affecting the environment in which competitors operate. It is the realization of principles of self-synchronization and speed of command.

The focus of EBO is not on a sequence of events, as in traditional attrition warfare. Rather, it is on operations in the cognitive domain, which in turn affect the physical. In Vietnam, the United States won every major battle yet lost the war – first in the cognitive domain, then in the physical domain. In Somalia, U.S. Rangers suffered a tiny fraction of the casualties sustained by the Somalis in a fire fight in Mogadishu, yet the U.S. forces abandoned the field and withdrew from the country. On September 11, 2001, a handful of terrorists commandeered three airplanes and changed the attitude of a nation. The *effects* of these asymmetric operations vastly surpassed the *events.*

Figure 3, adapted from the 2001 C4ISR Cooperative Research Program (CCRP) / American Institute of Aeronautics and Astronautics (AIAA) Workshop on Sensemaking, cited in [9], illustrates areas of vulnerability in the cognitive domain as decision makers process information.

"Next, observers will fuse the information on the situation with inputs from other levels and arenas to create a bigger picture of the situation," explains Dr. Ed Smith, a senior analyst on *Network Centric Effects Based Operations* at Boeing. "In so doing, they will attempt to put this picture into a wider temporal, spatial and situational context by comparing it with other information such as a history of similar actions in the same area over time. Finally, they will attempt to make some sense of this picture in light of a personal experience base that includes education, training, culture and personality, but that may also be affected by physiological factors such as a lack of sleep." [9]

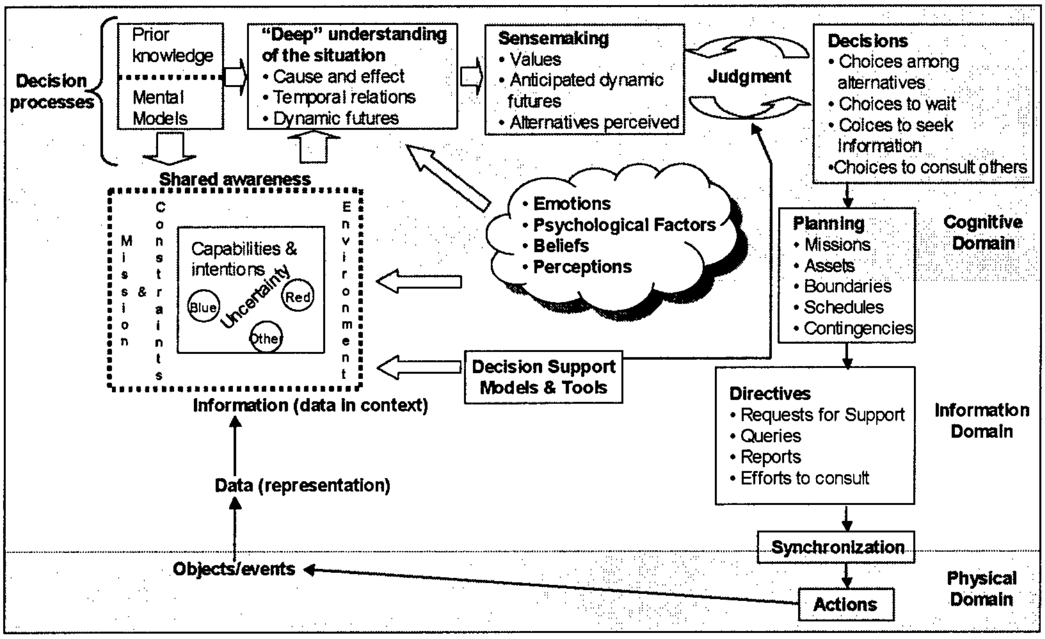


Figure 3: Operations in the Cognitive Domain [9]

1.4. Network-*Centric* Versus Network-*Enabled* Systems

Network-centric systems have unique qualities that differentiate them from other types of systems, and they range in application to far more than the information technology (IT) sector alone. The operation of a highway network, for example, demonstrates characteristics of an NCS, with autonomous nodes (vehicles) interacting with a common purpose (efficiently getting to individual destinations) and sharing a common relevant operating picture (traffic and weather conditions). A naval fleet also shares these qualities. Both of these examples span centuries of history and may be considered "low technology."

"Network centric" gained popularity as a term based on the works of Cebrowski, Alberts, Garstka and Stein referenced earlier. In many venues, however, it is used more broadly to describe systems that are *information-enabled* or *network-enabled.* The British Ministry of Defence (MoD) view of network-centric warfare, as stated in 2002, is of a system *enabled* by the networking of information. "The network is an enabler, not an answer," declared Lt. Col. David Turner of the MoD Directorate of Land Digitization. "The conduct of warfighting remains the same." [11]

This evolutionary use of technology to do the same things faster, rather than a revolutionary change to do things differently, helps to distinguish *enabled* from *centric* systems. The evolution of communications from face-to-face speech to smoke signals, to flags, to radios, to satellites does not describe a network-*centric* system – only one that is more efficiently network-*enabled.* These distinctions bear clarification.

A *system* is a set of interrelated components working together toward some common objective or purpose, according to Blanchard and Fabrycky. [12] In *Systems Engineering and Analysis,* they note that these components – the operating parts of the system consisting of inputs, processes, and outputs – have the following properties:

- The properties and behavior of each component of the set has an effect on the properties and behavior of the set as a whole.
- The properties and behavior of each component of the set depends on the properties and behavior of at least one other component in the set.
- Each possible subset of components has the two properties listed above; the components cannot be divided into independent subsets.

Further, each system component may assume a variety of values to describe a system state as set by some control action and one or more restrictions.

Finally, they state that systems are also composed of *attributes*, the properties or discernable manifestations of the components that characterize the system, and *relationships*, the links between components and attributes.

A key concept in differentiating network-enabled from network-centric systems is in the difference between a *relation* and a *system*. Blanchard and Fabrycky [12] point out three major differences between the two:

1. A relation exists between two and only two components, whereas a system is described by the interaction between many components.

2. A relation is formed out of the imminent qualities of the components, whereas a system is created by the particular position and spatial distribution of its components. The components of a relation are separated spatially, whereas a system is made up of the interacting distribution of its components.

3. The connection between the components of a relation is direct, whereas the connection in a system depends on a common reference to the entire set of components making up the system.

Figure 4 illustrates a network-enabled system. The network, though complex and able to map to any system, is merely an enabler for independent systems, which are end points unto themselves, each possessing a distinct and independent capability or function. Although a faster, more efficient network may allow nodes to communicate more quickly with various other nodes, it remains a *sequential* process.

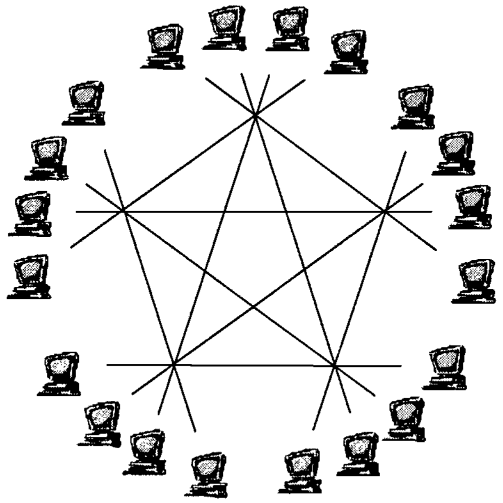


Figure 4: A Network-Enabled System

Network-enabled systems follow the relation model, albeit possibly on a large and complex scale. The British vision described by Turner is one "linking sensors, decision-makers and weapon systems so that information can be translated into synchronized and overwhelmingly rapid military effect." [11] He sees the network as enabling the rapid flow of information to the existing command and control structure. "What can we do more with what we've already done?" he asks.

A network-centric system follows the system model, the Internet being the quintessential example. The Internet is a vast web of entities knowledgeable about a relatively small number of networked components attached to it. It is unconcerned with *what* is transmitted (events) but is focused on *how* to move messages to their intended recipients (effects). Figure 5 illustrates such a system.

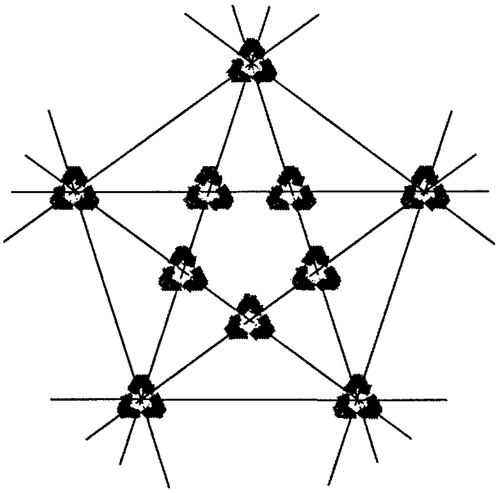


Figure 5: A Network-Centric System

In a network-centric system, the network is analogous to a biological central nervous system, and nodes to operational parts of the body. All nodes interact with and are interdependent on all others. Each must manage its own function, but only within the constraints imposed by all others, singularly and collectively, for total system success.

1.5. Summary of Attributes for Network-Centric Systems

A network-centric system, then, can be viewed as a class of systems – inheriting the properties of and meeting the criteria for a system as described above – that displays these additional attributes:

a. It is a network of knowledgeable nodes that share a common relevant operating picture and cooperate in a shared common environment.

b. Functional nodes reside in the cognitive, physical and information domains and communicate with each other and between domains.

c. The network is the NCS central nervous system: gathering, analyzing, and managing information that continuously stimulates the system.

d. Knowledgeable nodes may act autonomously (self-synchronization) with or without a central command and control facility.

1.6. Endnotes

[1] J. Hazlett, "Just-In-Time Warfare," in *Dominant Battlespace Knowledge*, M. C. Libicki, Ed.: National Defense University Press, 1995.

[2] D. S. Alberts, J. J. Garstka, and F. P. Stein, *Network Centric Warfare*, Second ed. Washington DC: CCRP, 2000.

[3] F. P. Stein, "Observations on the Emergence of Network Centric Warfare," presented at 1998 Command and Control Research & Technology Symposium, 1998.

[4] "Network Centric Warfare: Department of Defense Report to Congress," Department of Defense, Washington, 27 July 2001.

[5] V. A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings*, 1998.

[6] J. R. Boyd, *A Discourse on Winning and Losing*. Maxwell AFB, AL: Air University Press, 1987.

[7] T. P. M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Naval Institute Proceedings*, 1999.

[8] D. Ozolek, "U.S. Transformation in the Age of Complexity: Establishing a Common Joint Context," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

[9] E. A. Smith, "From Network Centric to Effects-based Operations," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

[10] USJFCOM, "Joint Forces Command Glossary," vol. 2002: United States Joint Forces Command, 2002.

[11] D. Turner, "Network Centric Warfare: The British Army's Aspirations," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

[12] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 1998.

Chapter 2. Network-Centric System Risk

This chapter describes the NCS Risk Taxonomy [13], with considerations for a hypersonic interceptor system. It builds on the architecture of network-centric systems presented earlier to meet the needs of these emerging NCS in the Information Age.

The NCS Risk Management Cycle is an iterative process, as shown in Figure 6. The common relevant operating picture (CROP) is the collective consciousness of the NCS and reflects total situation awareness, both internal and external. Continuous risk assessment occurs at both the NCS and node levels, with action plans developed by and negotiated between nodes.

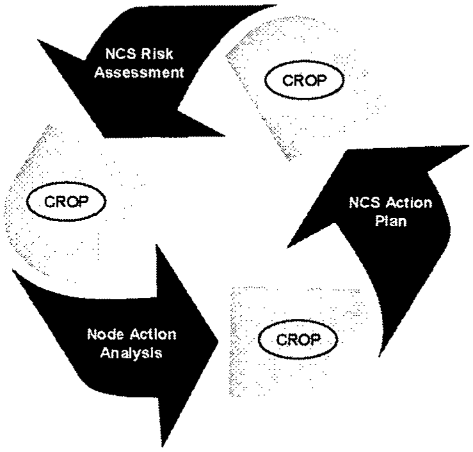


Figure 6: The NCS Risk Management Cycle

2.1. Risk, Risk Analysis, and Risk Management

The Army defines *risk management* as "the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits." [14]

Risk is often defined as the probability and severity of adverse effects. [15] It is measured as the combined effect of the probability of occurrence and the assessed consequences given that occurrence. [16]

Identifying risks comes in the form of determining sources of risk events and situations under which they may occur. [17] *Risk analysis* includes the process of determining the probability of occurrence and the magnitude of the consequence. Blanchard and Fabrycky note that the final phase, *risk abatement*, involves techniques to control, reduce or eliminate risk. [16]

Buede [18] notes that several strategies exist for dealing with risk: *Risk avoidance*, the selection of apparent low-risk alternatives to avoid a risk event occurrence; *risk transference*, transferring risk to others, as with an insurance policy; and *risk management*, the use of fallback options in case a riskier option fails. In the context of this research, each of these falls within the purview of risk abatement as defined by Blanchard and Fabrycky and is considered part of the risk management process.

U.S. Department of Defense guidance for risk management in the acquisition process specifies that, "Program risk includes all risk events and their relationships to each other. It is a top-level assessment of impact to the program when all risk events at the lower levels of the program are considered." It continues, "One of the greatest strengths of a formal, continuous risk management process is the proactive quest to identify risk events for handling, and the reduction of uncertainty that results from handling actions." [19]

2.2. NCS Risk Taxonomy

A systems approach to NCS requires that the scope of risk assessment be extended to account for a broad range of factors. Such a framework must be sufficiently robust to apply to all network-centric systems while being adequately specific to provide a quantifiable assessment.

The NCS Risk Taxonomy is presented to further define the nature of NCS risk and to establish a structure for NCS risk assessment. The complete structure is shown in Figure 7 and described by domain and factor in the following sub-sections.

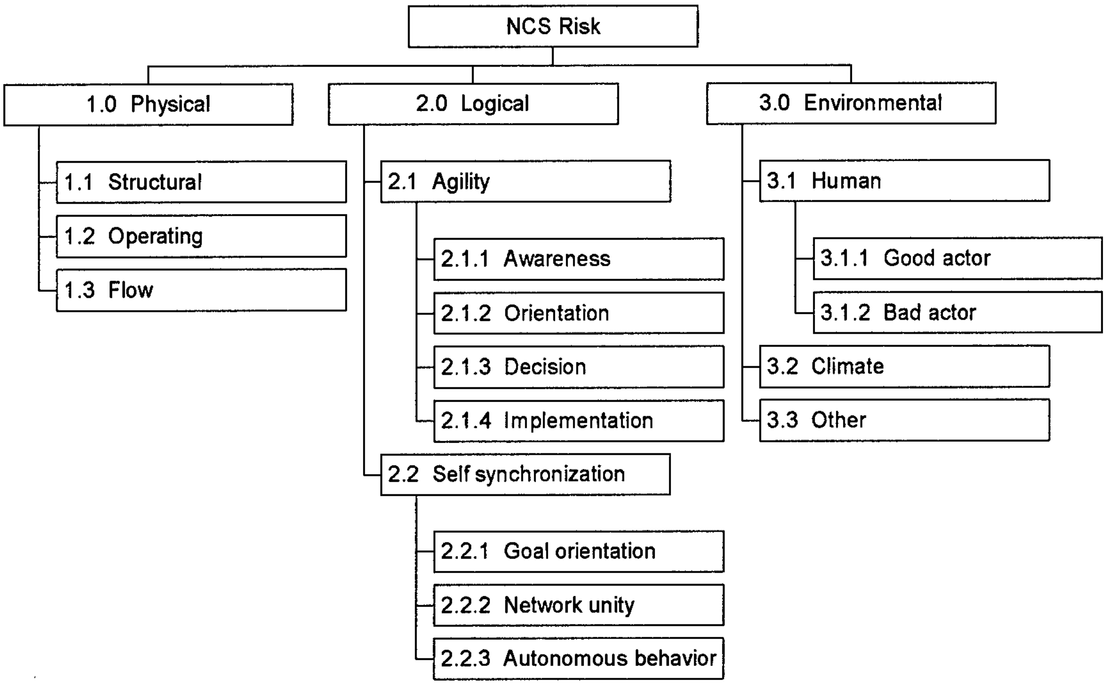


Figure 7: The NCS Risk Taxonomy

2.3. NCS Risk Domains

Effective collaboration within NCS has special challenges in a military environment that is complex, dynamic, and fluid and is characterized by uncertainty, ambiguity, and friction. The incorporation of robotic actors such as HSIs adds greater complexity to a comprehensive and coordinated decision-making process.

A network-centric system is separate from an information-enabled system and therefore has vulnerabilities beyond those of information assurance. Yet much of the work on Information Age systems has focused on just that. Given that network-centric systems exist and are distinguishable as a class of system, the task of managing risk to them must be viewed from a holistic, systems approach.

The Army defines risk management as "the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits." [20] War, it states, is inherently complex, dynamic and fluid and is characterized by:

- **uncertainty** arising from unknowns or a lack of information,

- **ambiguity**, the blurring or fog that makes distinguishing between fact and impression about the situation and the enemy difficult, and
- **friction**, resulting from change, operational hazards, fatigue, and fears brought on by danger.

Concerns facing decision makers while operating in such an environment, the Army says, include:

- analyzing the factors of enemy, terrain, troops and time available (METT-T) to determine both tactical and accidental risks and appropriate risk reduction measures,
- determining the correct units, equipment composition, and sequence,
- identifying controls essential to safety and environmental protection.

These challenges to mission success are heightened in an NCW environment where autonomous, often robotic actors operate in a highly decentralized context within a rapidly developing, uncertain situation. Managing risk to an NCS requires decision makers to anticipate threat activity with sufficient lead time to not only survive, but to control the threat's decision cycle, while simultaneously managing the immediate situation.

NCS risk domains organize factors from across operational lines into a risk hierarchy, as shown in Figure 8.

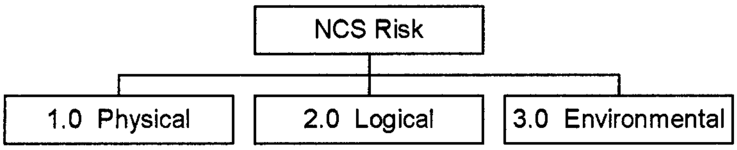


Figure 8: NCS Risk Domains

2.3.1. The Physical Domain

Physical factors are the tangible components of the system, as shown in Figure 9.

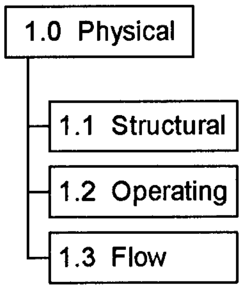


Figure 9: NCS Physical Factors

- *Structural components* are those that normally do not change during the life of a system. The frame of a car, an airport terminal, and the wiring that brings electricity into the home are examples.

- *Operating components* are those that process material to make the system function. The car's engine and transmission, the airport's traffic control system and baggage carousels, and the power company's generators and transformers are examples of these components.

- *Flow components* are materials processed through the operating components. These are often expendables such as fuel, but may be other systems such as airplanes, baggage or people.

2.3.2. The Logical Domain

Logical factors include all cognitive functions of the NCS, whether by software or by human intervention. As seen in Figure 10, they focus on the two main tenets of NCS – *Agility* and *Self-Synchronization* – as described in Chapter 1.

- *Agility*. This embodies the *speed of command* principle of network-centric warfare. It is the effect enabled by that principle and applied to all NCS. The term was used in the U.S. Army's AirLand Battle doctrine of the 1980s and '90s to describe "the first prerequisite for seizing and holding the initiative." [21] It is "the ability of friendly forces to act faster than the enemy," the Army said. "Such greater quickness permits the rapid concentration of friendly strength against enemy vulnerabilities. This must be done repeatedly so that by the time the enemy reacts to one action, another has already taken its place, disrupting his plans and leading to late, uncoordinated, and piecemeal enemy responses."

- *Awareness* is the degree of comprehending the common relevant operating picture (CROP). In this arena, what nodes *need* to know is "pushed" to them, according to the U.S. Joint Forces Command, and what they *want* to know is "pulled." [8] Observations from an Army division-level advanced warfighting experiment (AWE) indicate that "good," not perfect intelligences mixed with clear commander's intent allows commanders to take prudent risks to achieve tactical advantage. [22]

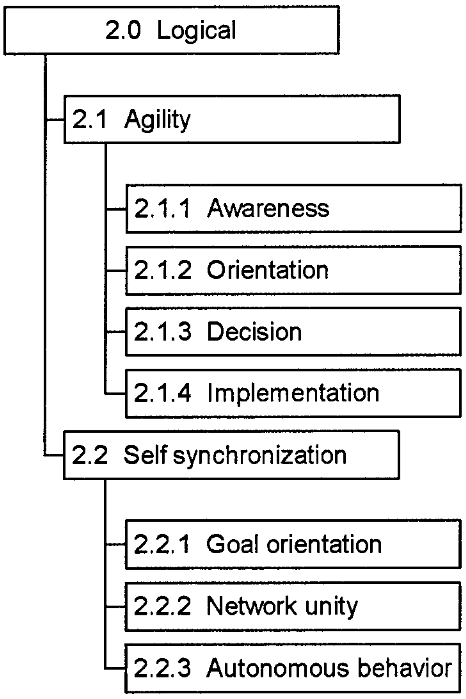


Figure 10: NCS Logical Factors

- *Orientation* is the degree of comprehending the situation given a level of training, education and experience. Webster defines "orientation" as the state of being oriented, or set right by adjusting to facts or principles; to acquaint with the existing situation or environment. [23] It is a critical piece of the observe, orient, decide, act (OODA) loop described in Chapter 1.

  - *Decision* is the degree to which cognitive comparisons can be made. Buede defines a decision as the "irrevocable allocation of resources to affect some chosen change or the continuance of the status quo." [18] He states that there are three major elements of the decision process:

    - Creative generation of alternatives.
    - Identification and quantification of multiple conflicting criteria.
    - Assessment and analysis of uncertainty about the situation.

    Each of these may be a source of failure.

  - *Implementation* is the degree to which an action can be taken as a result of a decision. In developing the OODA loop model, Boyd [6] points out that "orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window."

- *Self synchronization*, as defined in Chapter 1, is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. [24] When applied to the broader class of network-centric systems, its functions take on a slightly different flavor, although the principles remain the same.

  - *Goal orientation* is the degree of comprehending the desired end state – the result, or effect – of the process. In military jargon it is the *commander's intent* and includes not only the mission, but also key tasks to be accomplished so that sub-elements understand intermediate goals and can act autonomously when unexpected situations arise. The Army describes this intent as "a clear, concise statement of what the force must do to succeed with respect to the enemy and the terrain and to the desired end state." [25] It does *not* include the *why*, the *how*, or the level of acceptable *risk* related to the process.

- *Network unity* is the degree to which nodes in the NCS can function *collectively* to achieve the goals of the system by maintaining network integrity. This provides the unity of effort described for NCW.

- *Autonomous behavior* is the degree to which nodes in the NCS can function *independently* to achieve system goals given a clear understanding of the mission, a common relevant operating picture, clear goal orientation, and a clear set of rules to bound the decision space.

2.3.3. The Environmental Domain

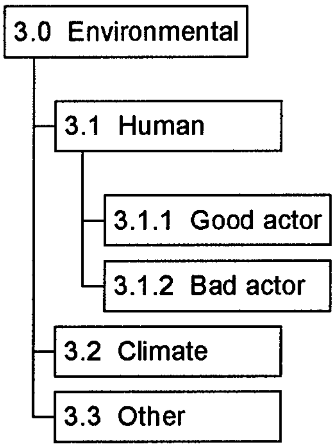
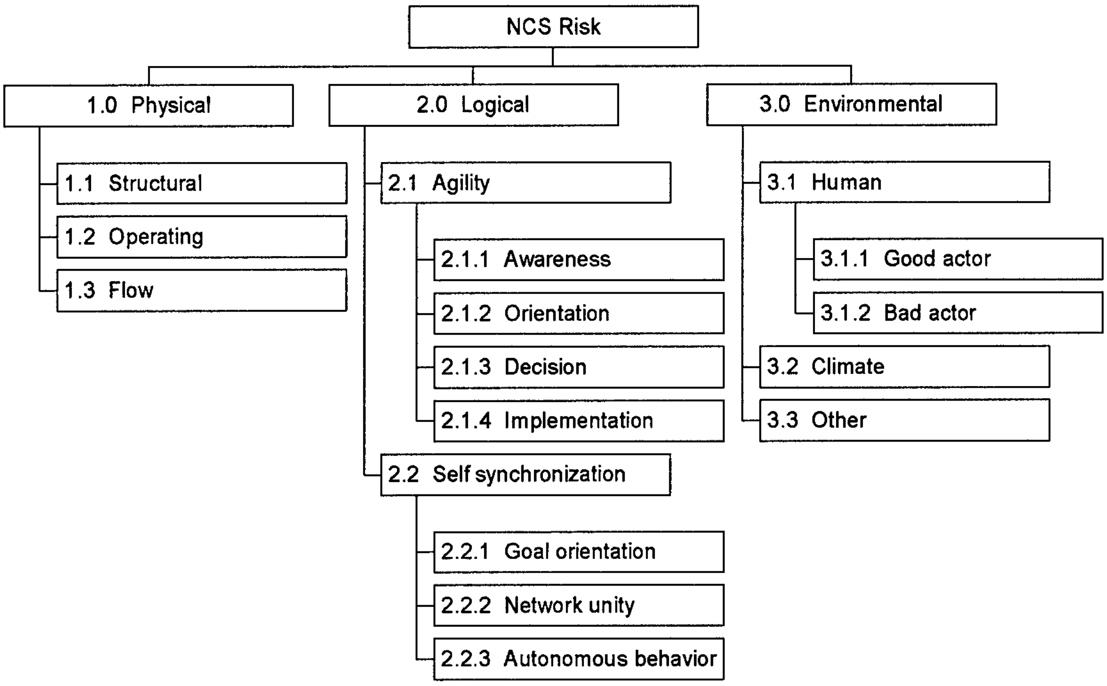


Figure 11: NCS Environmental Factors

The earlier review of failure sources revealed that external sources play a vital role in network-centric systems. Figure 11 shows these external factors in an NCS environment.

- *Human* components include all interactions with people, regardless of motivation.
  - *Good Actor* is the degree to which well-intentioned humans contribute to the desired functioning of the system.
  - *Bad Actor* is the degree to which mal-intentioned humans contribute to the desired functioning of the system.



- *Climate* is the degree to which non-human elements contribute to the desired functioning of the system. These elements include, but are not limited to, weather, heating, ventilation and air conditioning (HVAC), and natural phenomena such as earthquakes, floods and volcanoes.

- *Other* is the degree to which external factors unique to the NCS contribute to the desired functioning of the system.

2.4. Endnotes

[13] P.D. West, *Dynamic Risk Management of Network-Centric Systems*, Ann Arbor, MI; ProQuest, 2003.

[14] U.S. Army, *FM 100-14: Risk Management*, Washington, DC, 1998.

[15] Y. Y. Haimes, *Risk Modeling, Assessment and Management*. New York: John Wiley & Sons, Inc, 1998.

[16] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 3rd ed.

[17] A. P. Sage, *Systems Engineering*. New York: John Wiley & Sons, Inc, 1992.

[18] D. M. Buede, *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons, Inc, 2000.

[19] E. A. Smith, "Network-Centric Warfare; What's the Point?" *Naval War College Review*, vol. Winter 2001, 2001.

[20] U. S. Army, "FM 100-14, Risk Management," U.S. Army Training and Doctrine Command, Ft. Monroe, VA, 23 April 1998.

[21] U.S. Army, *FM 100-5: Operations*. Washington, DC, 1986.

[22] F. Stein, "NCW: Warfighting Insights from Experimentation," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

[23] *Webster's Ninth New Collegiate Dictionary*, 9th ed. Springfield, MA: Werriam-Webster, Inc, 1984.

[24] V. A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings*, 1998.

[25] U.S. Army, *FM 101-5 Staff Organization and Operations*. Washington: Department of the Army, 1997.

Chapter 3. Risk Assessment by Network-Centric Systems

Nodes in a network-centric system must continuously evaluate risks to consider their actions in the current and near-term situations. For a network-centric system such as the Internet, a causative event could be the introduction of a computer virus by a Bad Actor. Outcomes could include infected systems and network security alerts. The virus could reach a system through the multiple exposure pathways of other nodes in the network, each of which could have a different probability of success depending on the vulnerability of the nodes to the attack.

As part of a decision support system for NCS, detailed probability assessments can help nodes plan for contingencies. For example, a knowledgeable node (ship) of a naval fleet at sea can consider a causative event such as a missile attack, with possible outcomes of one or more missile detonations, with exposure through physical, logical, or environmental pathways.

3.1. Exposure and Consequence Probabilities

Risk exposure is the vulnerability to outcomes through one or more pathways. Rowe [26] states that *causative events* and *outcomes* without *exposure* poses no risk and therefore are best assessed through hypothesis testing, experimental design and experimentation.

Pathways for the network-centric system include all of the nodes making up the system. Each node has a degree of vulnerability from zero to 100 percent to any threat. Calculating risk exposure then becomes a reliability problem. The process is shown in Figure 12, where P_{x1}

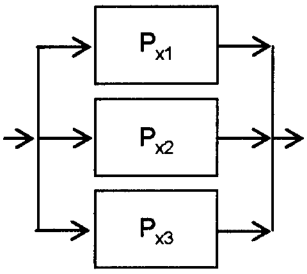


Figure 12: Exposure Flow

through P_{xn} represent the probabilities that the system's nodes will be affected by the threat. These are drawn from the NCS Risk Taxonomy for each sub-system (node).

Exposure for the system in Figure 12 is calculated in Equation 1.

$$\text{P(Exposure)} = 1 - (1 - P_{x1})(1 - P_{x2})(1 - P_{x3}) \tag{1}$$

Equation 1: Risk Exposure Through Multiple Pathways

If, for the Internet example, the vulnerability of each of three machines in an NCS is derived from the NCS Risk Taxonomy to be 0.83, 0.42, and 0.37, respectively, the total exposure to the system is calculated in Equation 22 to be 0.55.

$$\text{P(Exposure)} = 1 - (1 - 0.83)(1 - 0.42)(1 - 0.37) = 0.94 \tag{2}$$

Equation 2: Risk Exposure Calculation

This approach to calculating pathway values differs from Rowe's, who views outcomes to be distributed across all pathways, so that the magnitude of the effect sums to unity and the magnitude of the pathways cannot exceed that of the outcome. Floodwater, for example, would be distributed across all available channels (pathways), although the magnitude of the flow would not be uniformly distributed. There also is an associated probability that the flow would take any given channel. This approach is less useful for NCS risk since the magnitude of the threat may be 100 percent for any one or more nodes.

The probability of a consequence affecting the system is the product of the probabilities of the event, the outcome, and the exposure, which can be solved as a combined series-parallel network reliability problem. This is shown graphically in Figure 13 and mathematically in Equation 3.

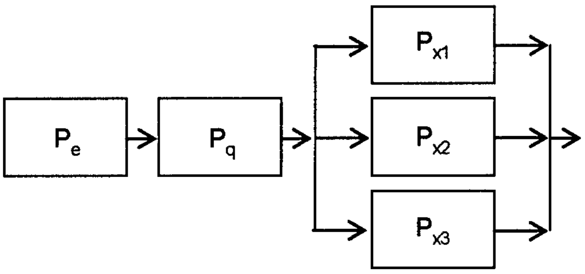


Figure 13: Consequence Probability Flow

$$\text{P(Consequence)} = (P_e)(P_q)[1 - (1- P_{x1})(1- P_{x2})(1- P_{x3})] \tag{3}$$

Equation 3: Consequence Probability Calculation

If the probability of a virus attack is 0.80, the likelihood that a virus would function correctly is 0.99, and risk exposures through multiple pathways are 0.83, 0.42, and 0.37, then the probability that an infection would affect the system can be calculated as in Equation 4.

$$\text{P(Consequence)} = (0.80)(0.99)[1 - (1- 0.83)(1- 0.42)(1- 0.37)] = 0.74 \tag{4}$$

Equation 4: Consequence Probability Example

3.2. DRMM Consequence Value Model

Factors identified in the NCS Risk Taxonomy all contribute to overall system risk, but not necessarily in equal measure in all circumstances. Identifying and applying appropriate risk mitigation actions depends not only on the likelihood that a factor will be affected, but also on the perceived value of that factor to the NCS mission at hand.

The NCS Risk Taxonomy can be viewed as the foundation for an objectives hierarchy pertaining to sources of failure in network-centric systems. The relationships of sub-element impacts are shown in Figure 14.

Missing from the tree in Figure 14 are directions of preference and a level of decomposition to where evaluation measures can be defined. It must therefore include at least one additional level to be complete, the composition of which is system-dependent – both measurable attributes and directions of preference will vary between network-centric systems. For example, *Flow*, defined earlier as materials processed through the operating components, may be measured as network data packets per second in an Internet application, in which more may be better, or it may refer to gallons of fuel expended per hour in an FCS node, in which less may be better.

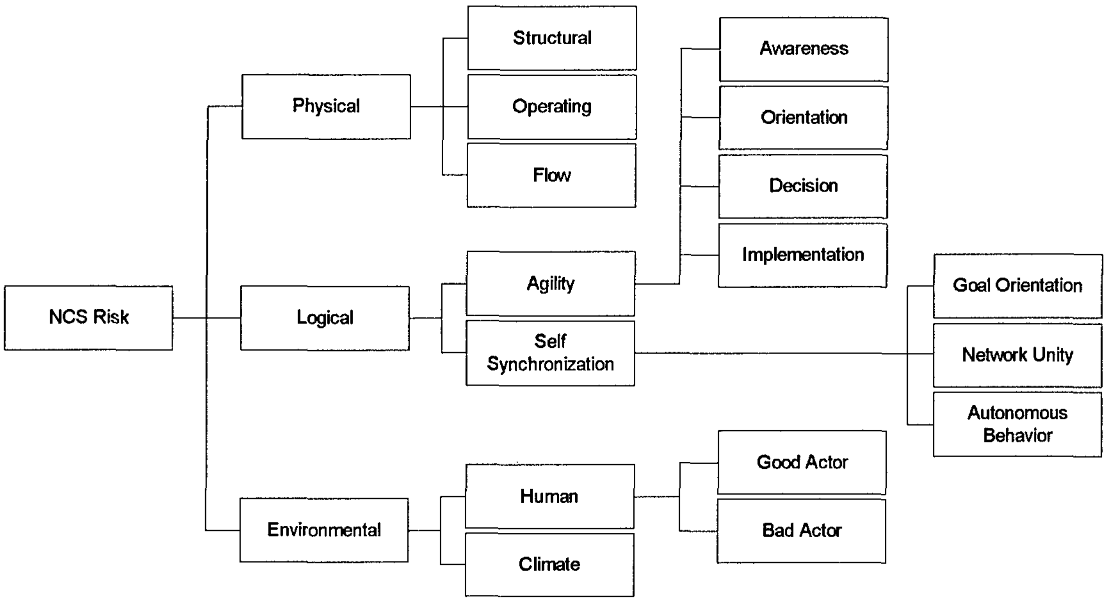


Figure 14: NCS Risk Taxonomy as an Objectives Hierarchy

No single method for assigning consequence values would apply to all NCS. In a military context, a single decision maker, the commander, may provide adequate breadth of decision making. In environments where multiple decision makers contribute, brainstorming approaches such as the Delphi method may be appropriate. This method consists of a series of repeated interrogations, usually by means of questionnaires, of a group of individuals whose opinions or judgments are of interest. Subsequent interrogations are accompanied by information regarding the preceding round, usually presented anonymously. Individual are encouraged to reconsider and, if appropriate, to change their previous replies in light of the replies of other members of the group. After two or three rounds, the group position may be determined by averaging.

As an example, consider the following scenario. Figure 15 represents a risk hierarchy for a military logistics supply point for fuel. There is a threat of terrorist attack and the commander has assigned relative consequence factors to each intermediate risk category (objective) using the method described earlier.

Each intermediate level of the tree is a decomposition of the level above it and must sum to unity. The global weights (GW) at the far right are the products of local weights (LW) applied by the decision maker. A globally-weighted value of 0.34 for *Gallons lost*, for example, is the

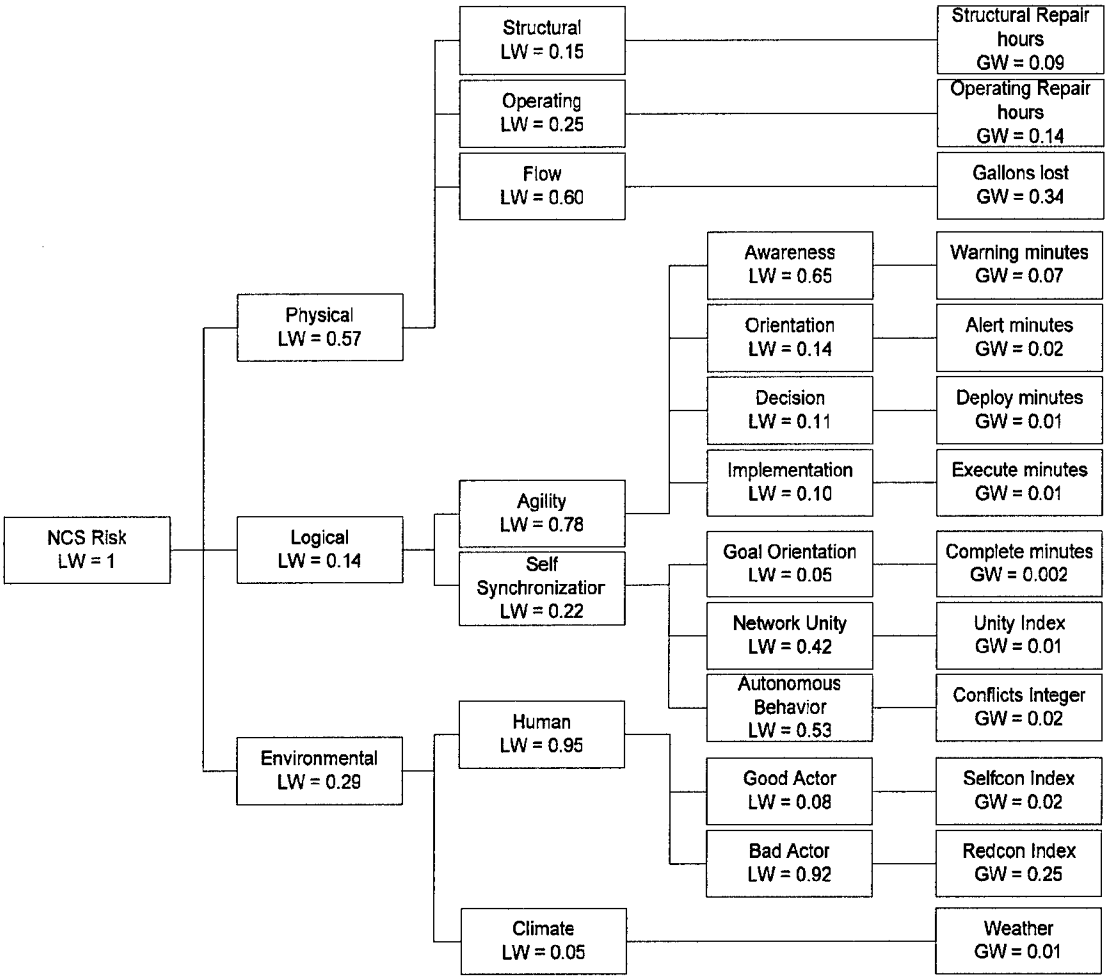


Figure 15: Risk Hierarchy for Fuel Depot Scenario

product of the decision maker's assessment for the *Physical* (0.57) and *Flow* (0.6) intermediate objectives. The global weights also sum to unity and represent the distribution of the decision maker's total risk assessment.

The tree reflects the decision maker's concern that fuel supply (flow component) and terrorists (bad actors) are the greatest sources of failure to the successful operation of the depot as a system, given this risky situation. Values used in this example are notional for the purpose of the scenario.

Simple, measurable attributes have been added to complete the hierarchy for the purpose of illustration. These are defined in Table 1.

Table 1: Attributes for Fuel Depot Scenario

Parent	Attribute	Units	Description
Structural	Structural Repair	Hours	Number of hours required to place structural components back into operation following a catastrophic failure.
Operating	Operating Repair	Hours	Number of hours required to place machinery back into operation following a catastrophic failure.
Flow	Gallons lost	Gallons	Number of gallons of fuel that may be lost in an attack.
Awareness	Warning	Minutes	Number of minutes of advance warning provided through the common relevant operating picture.
Orientation	Alert	Minutes	Number of minutes from the time of attack to the time of alert, reflecting comprehension of the situation.
Decision	Deploy	Minutes	Number of minutes from the time of alert to the time of an "irrevocable allocation of resources to affect some chosen change or the continuance of the status quo." [6]
Implementation	Execute	Minutes	Number of minutes from the time of the decision to deploy to the start of the execution of that decision.
Goal Orientation	Complete	Minutes	Number of minutes from time of execution to the time the remediation plan is complete, reflecting comprehension of the goal and the intermediate steps required to achieve it.
Network Unity	Unity	Index Number	Number from 0 to 1 reflecting the degree of NCS functional and organizational integrity.
Autonomous Behavior	Conflicts	Integer	Number of conflicts between other nodes that must be resolved before action can occur.
Good Actor	Selfcon	Index Number	Own self readiness condition index; a composite index
Bad Actor	Redcon	Index Number	Estimate of threat readiness condition; a composite index

Climate	Weather	Index Number	Index of expected effects of weather factors including temperature, humidity, precipitation, wind

Lowest-level attributes may vary by both NCS and risk situation. They should avoid prescribing solutions, such as by using *number of soldiers*, which limits the set of feasible alternatives to only those that include soldiers.

3.3. Analysis of Alternatives

Given the autonomous nature of network-centric systems, human-intensive alternative generation techniques such as brainstorming, mind-mapping, dynamic confrontation, or Delphi may be too costly to develop. However, to function autonomously an NCS node must have an existing behavioral rules base. By extending the rules base, a node can address the three questions posed above by Haimes. How well it can do so is dependent on node capabilities.

An underlying set of behaviors is built into every NCS node. Many other systems have them in the form of standing operating procedures (SOPs). In an Army tactical unit, for example, a *Tactical SOP* prescribes each entity's role both individually and as a member of a team, whether the entity is a soldier or a combat vehicle. This allows soldiers to be interchangeable between units with minimal loss of efficiency.

The SOP provides the baseline, or "do nothing" alternative for conducting a mission. Given no change in the system's original situation, doing nothing outside of SOP should result in mission success. Developing and controlling situations, however, enables the NCS to get inside the competition's OODA loop and gain competitive advantage. A rapid, efficient method for identifying or generating feasible alternatives is necessary.

3.3.1. Analysis of Alternatives

A value-focused approach, as described in Chapter 2, explores available alternatives appropriate for the decision maker's values. A recap of values for the example scenario is highlighted in Table 2.

Table 2: Fuel Deport Scenario Attribute Weights

Failure Source	Attribute	Weight
Structural	Repair time	0.09
Operating	Repair time	0.14
Flow	Gallons lost	0.34
Awareness	Warning time	0.07
Orientation	Alert time	0.02
Decision	Deploy time	0.01
Implement	Execute time	0.01
Goal Orientation	Complete	0.002
Unity	Unity	0.01
Autonomous	Conflicts	0.02
Good Actor	Selfcon	0.02
Bad Actor	Redcon	0.25
Climate	Weather	0.01

When viewed as a cumulative distribution, shown in Figure 16, it is clear that only a few attributes account for much of the total distribution. Using the Pareto Principle to separate the vital few from the trivial many, cutoffs can be set to consider only those attributes that dominate.

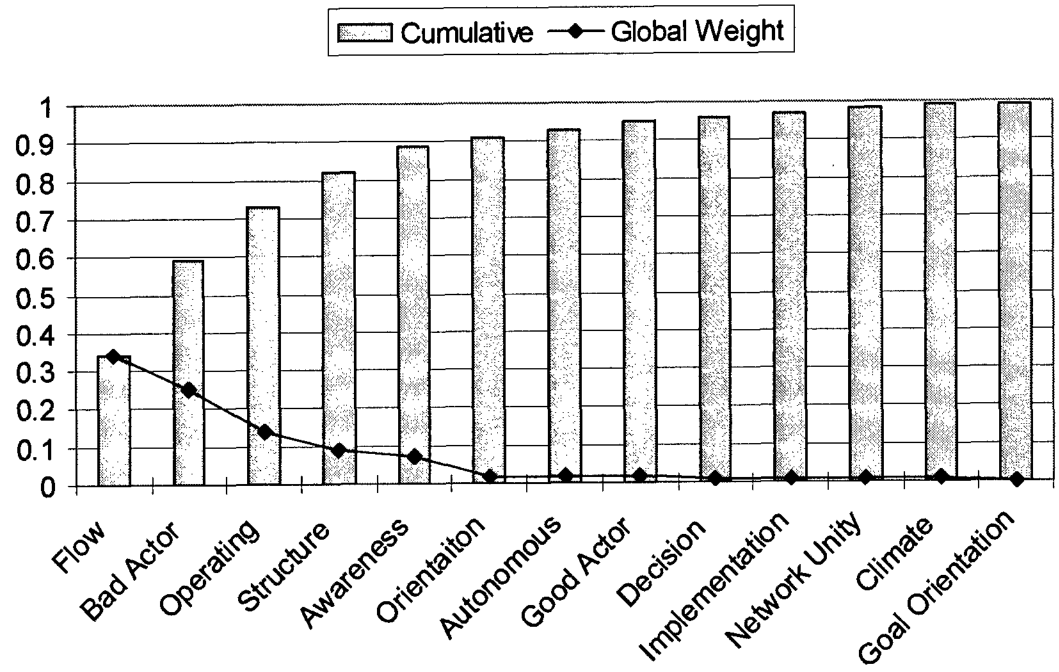


Figure 16: Cumulative Distribution of Weights, Fuel Depot Scenario

This view helps determine the number of alternatives that need to be generated before a decision can be made. More complex approaches such as those by Starr and Greenwood [27] and Zeleny [28] may be too calculation-heavy to work well in an operational environment. Starr and Greenwood's approach uses the cumulative entropy of successive alternatives to determine the number to consider. It is based on the idea that as the generation process progresses, the degree to which alternatives are different eventually reaches a point of insignificance. This point is set arbitrarily by the decision maker. In the latter instance, Zeleny uses the Euclidean distance between alternatives and an "ideal," which is the intersection of the technological boundaries with respect to the criteria. The generation process stops when the distances between alternatives become insignificant or when a boundary is met. Again, the determination of insignificance is set arbitrarily.

The global weight line in Figure 16 shows a practically insignificant contribution from Orientation to Goal Orientation. Limiting the generation of alternatives to only those "vital few" that are feasible, given the capabilities of the system, will limit the set of alternatives for evaluation to a reasonable size.

In the fuel depot scenario, if the decision maker wants to consider only top contributors that make up 80 percent of the risk, then alternatives need only be considered for Flow, Bad Actors, and Operating component risks. Flow and Operating components are children of the Physical component, so alternatives should focus on the physical protection of the fuel and the equipment that processes it (a coordinated alternative with *Operating* GW 0.14 and *Flow* GW 0.34). The decision maker is then faced with two objectives:

1. Protect the fuel and equipment (combined global weight 0.48).
2. Defend against the terrorist attack (global weight 0.25).

This approach capitalizes on Keeney's concept of value-focused thinking (VFT) to reduce the risk management strategy to a small number of relevant alternatives. If a node has no weapons or other means to defend against attack, the solution set is empty and the node can take no action. If the node also cannot meet the first objective, then it continues to function according to SOP unless there is intervention by a higher decision maker. It was noted in Section 1 that a network-centric system *could* act autonomously, but also could be subject to human intervention.

3.3.2. Determining Alternative Utility

Decision-making occurs after attribute weights are determined and feasible alternatives identified. Raw measures of merit (effectives or performance) are converted to utility values (utiles) that are weighted by the global weights of appropriate attributes and summed to achieve a total utility score. For a single decision maker, the alternative with the greatest total utility should be the preferred action. This is an intermediate step for a network-centric system, however, since multiple nodes will consider responses to a threat to the NCS. Given attributes of an NCS such as network unity and goal orientation, nodes must negotiate responses to ensure the NCS has the greatest chance of mission success.

Continuing the fuel depot scenario, consider an armed unmanned aerial vehicle (AUAV) in support of the depot (or an HSI in a future scenario). It receives the depot's weighted attributes through the common relevant operating picture (CROP). The AUAV creates the following feasible alternatives to answer the question: *What can be done?*

- Do nothing (continue per SOP).

- Fly over the fuel and equipment areas, engaging detected intruders.

- Broaden its current flight pattern to cover area vacated by another AUAV that that be executing another action.

The AUAV conducts a self risk assessment using a process similar to that of the depot. Table 3 shows a notional decision matrix for the AUAV considering the three alternatives identified earlier.

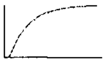
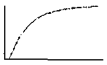
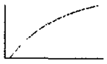
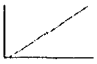
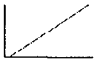
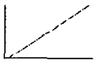
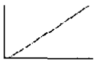
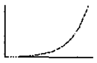
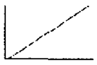
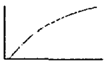
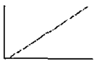
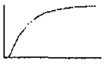
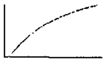
Values for the minimum acceptable thresholds (x^0), ideals (x^*), value curves, and raw scores are hypothetical for the example. Utiles were calculated by assigning the raw score to x in the corresponding value curve. Total utility for the alternative is the sum of the utiles after being weighted by the corresponding attribute weight, as shown in Equation 5.

$$U = \sum_{i=1}^{n} gw_i(u_i) \tag{5}$$

Equation 5: Calculating Alternative Utility

The alternative with the highest total utility would be the one selected by the AUAV and would be reflected to the NCS CROP. If communication were lost or if no further guidance were issued, the AUAV would begin execution of this plan while continuing to monitor the CROP for new information.

Table 3: Decision Matrix for an NCS Node

				Continue Mission		Attack		Expanded Defense	
		x^0	x^*	Raw	Utile	Raw	Utile	Raw	Utile
Structural Repair hours GW = 0.27		24	0	1	0.998	8	0.971	1	0.998
Operating Repair hours GW = 0.22		24	1	3	0.995	5	0.989	3	0.995
Fuel GPH GW = 0.12		10	2	3	0.956	5	0.825	6	0.731
Warning minutes GW = 0.02		30	0	20	0.333	20	0.333	20	0.333
Alert minutes GW = 0.02		1	0	0.30	0.30	0.50	0.50	0.20	0.20
Deploy minutes GW = 0.06		1	0	0.30	0.30	0.30	0.30	0.30	0.30
Execute minutes GW = 0.01		1	0	0.10	0.10	0.10	0.10	0.10	0.10
Complete minutes GW = 0.01		60	0	30	0.076	55	0.004	45	0.017
Unity GW = 0.01		0.75	1	1	1	0.80	0.20	0.90	0.60
Conflicts GW = 0.02		10	0	0	1	7	0.522	1	0.965
Selfcon GW = 0.02		0	10	9	0.90	2	0.20	7	0.70
Redcon GW = 0.12		10	0	8	0.636	2	0.988	9	0.396
Weather GW = 0.10		5	0	1	0.923	2	0.808	1	0.923
		Total Utility:			0.852		0.830		0.785

The basic decision model illustrated here is subject to variability at several points – from decision-maker risk assessment to risk attitude – that may affect the preferred alternative. Sensitivity of the decision to this variability should be considered. The decision to *continue mission* or *attack* is separated by only 0.02 in total utility and may be easily swayed be small changes in decision-maker values. Addition of a *sensitivity analysis* step is necessary to further refine the results.

3.4. Arbitrating Multiple Node Decisions

Development of an execution-time model for dynamic risk management of NCS described in this report focuses on functions necessary to apply the NCS Risk Taxonomy to real-time NCS operations. This section details steps at the node level to implement that model.

As described in Section 1, the Common Relevant Operating Picture (CROP) represents the collective consciousness of the NCS and is distributed to all nodes in the system. Each autonomous NCS node must consider both its current and developing situations and those of the larger system.

The primary alternatives from each node become the initial alternatives for the NCS-level decision process, starting the Mitigation Generation Phase. The value-focused thinking techniques for alternative generation and screening are then applied at the higher level and the top candidates are swing-weighted and globally-weighted using the same methods described here, but at the NCS level. It is possible that the *continue mission* alternative is overridden for the AUAV described above and the *attack* alternative is selected by the collective NCS as the one having the greatest NCS-level utility.

As each decision cycle initializes, nodes start with the current CROP, which includes the most recent assessments by all nodes. Given the same decision-making rules, every node should arrive at the same decision. However, faulty communication between nodes or other internal errors may cause the process to fail. If a node is lost, acts autonomously contrary to the NCS decision due to communication failure, or otherwise malfunctions, the CROP updates the operational picture in its continuous risk assessment and management process

3.5. Endnotes

[26] W. D. Rowe, *An Anatomy of Risk*. New York: John Wiley & Sons, 1977.

[27] M. K. Starr and L. Greenwood, "Normative Generation of Alternatives with Multiple Criteria Evaluation," in *Multiple Criteria Decision Making*, vol. 6, *TIMS Studies in the Management Sciences*. Amsterdam: North-Holland Publishing, 1977.

[28] M. Zeleny, *Multiple Criteria Decision Making*. New York: McGraw-Hill, 1982.

Chapter 4. Summary

This report describes the operation of network-centric systems in an asymmetric competitive environment and details a real-time, values-oriented risk management model within the NCS framework.

An NCS Risk Taxonomy is used to quantify overall system risk. This taxonomy identifies 13 critical risk factors common to all NCS:

- Structural
- Operating
- Flow
- Awareness
- Orientation
- Decision
- Implementation
- Goal Orientation
- Network Unity
- Autonomous Behavior
- Good Actor
- Bad Actor
- Climate

The NCS Dynamic Risk Management Model (DRMM) extends the Taxonomy to manage these risks while the NCS is in operation. It links risk management and decision analysis techniques to continuously guide NCS risk mitigation actions. The process occurs for each node in the network and for the NCS as a whole – it is conceivable that a less desirable action, from a node's point of view, may be taken if the benefit to the NCS outweighs the cost to the individual node, even if it means the destruction of the node.

Given the NCS objective of controlling speed of command and self-synchronization, the risk management model must be predictive in that it must assess developments far enough in the future so that appropriate actions have sufficient time to be executed. Finally, it must be dynamic and appear to be continuous so that "best" solutions are constantly available in real time.

With reliable access to the common relevant operating picture – fed by the intelligence gathering and reporting capability of sensor action nodes, a nearly continuous stream of risk assessments can be maintained. By updating the degree of situational uncertainty at regular intervals, threats can be tracked and likely scenarios predicted.

The DRMM consists of a Risk Analysis Phase, a Mitigation Generation Phase, and an Action Phase. A graphical representation of the model is shown in Figure 17.

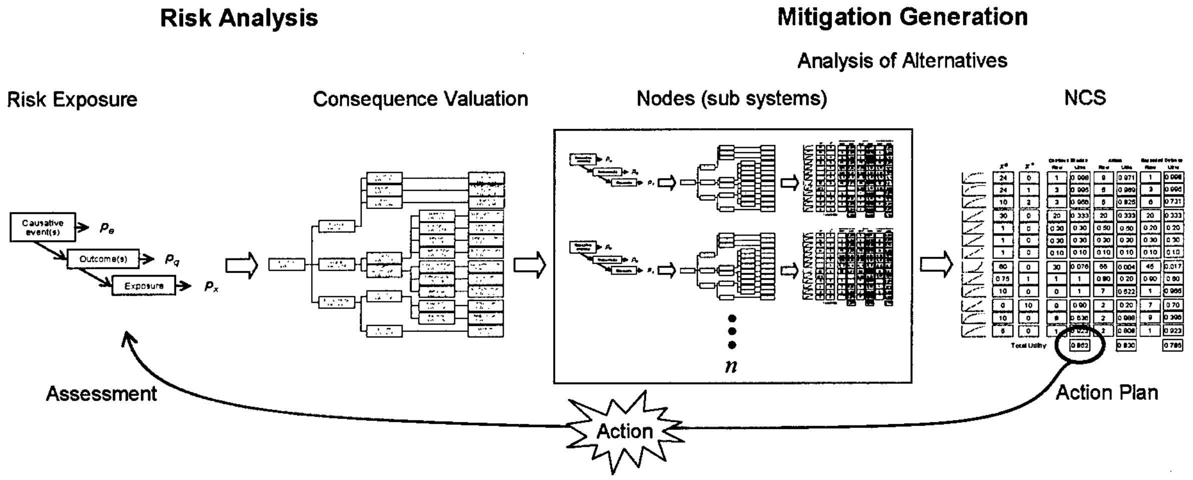


Figure 17: Graphical View of DRMM Process

The Risk Analysis Phase includes a risk exposure assessment and consequence valuation and is based on the NCS Risk Taxonomy developed in this chapter.

The Mitigation Generation Phase begins with individual nodes conducting their own risk assessments based on the greater NCS risk analysis. Using multi-attribute utility (MAU) analysis, each node generates and evaluates responses that it believes it can make. A preferred response is selected, which becomes the default action to be taken in case of loss of contact with the greater NCS. Nodes also maintain an NCS-level plan that is shared through the CROP. Node-level alternatives are consolidated as a preliminary NCS pool. The screening and evaluation process then repeats at the NCS level and an NCS-preferred alternative is selected and executed.

Preferred alternatives are executed in the Action Phase and the cycle continues. How frequently it repeats is dependent upon the NCS. It is a discrete event model, but is repeated at an appropriate rate so as to appear to be virtually continuous.

Chapter 5. Bibliography

Alberts, D.S., Garstka, J.J., and Stein, F.P., *Network Centric Warfare*, Second ed. Washington DC: CCRP, 2000.

Barnett, T.P.M., "The Seven Deadly Sins of Network-Centric Warfare," *Naval Institute Proceedings*, 1999.

Blanchard, B.S., and Fabrycky, W.J., *Systems Engineering and Analysis*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 1998.

Boyd, J.R., *A Discourse on Winning and Losing*. Maxwell AFB, AL: Air University Press, 1987.

Buede, D.M., *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons, Inc, 2000.

Cebrowski, V.A.K., and Garstka, J.J., "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings*, 1998.

Department of Defense, "Network Centric Warfare: Department of Defense Report to Congress," Washington, 27 July 2001.

Haimes, Y.Y., *Risk Modeling, Assessment and Management*. New York: John Wiley & Sons, Inc, 1998.

Hazlett, J. "Just-In-Time Warfare," in *Dominant Battlespace Knowledge*, M. C. Libicki, Ed.: National Defense University Press, 1995.

Ozolek, D., "U.S. Transformation in the Age of Complexity: Establishing a Common Joint Context," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

Rowe, W.D., *An Anatomy of Risk*. New York: John Wiley & Sons, 1977.

Sage, A.P., *Systems Engineering*. New York: John Wiley & Sons, Inc, 1992.

Smith, E.A., "From Network Centric to Effects-based Operations," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

Smith, E.A., "Network-Centric Warfare; What's the Point?" *Naval War College Review*, vol. Winter 2001, 2001.

Starr, M.K., and Greenwood, L., "Normative Generation of Alternatives with Multiple Criteria Evaluation," in *Multiple Criteria Decision Making*, vol. 6, *TIMS Studies in the Management Sciences*. Amsterdam: North-Holland Publishing, 1977.

Stein, F., "NCW: Warfighting Insights from Experimentation," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

Stein, F.P., "Observations on the Emergence of Network Centric Warfare," presented at 1998 Command and Control Research & Technology Symposium, 1998.

Turner, D., "Network Centric Warfare: The British Army's Aspirations," presented at Fourth Annual Conference on Network Centric Warfare, London, 2002.

U.S. Army, *FM 100-5: Operations*. Washington, DC, 1986.

U.S. Army, *FM 100-14, Risk Management,* U.S. Army Training and Doctrine Command, Ft. Monroe, VA, 23 April 1998.

U.S. Army, *FM 101-5 Staff Organization and Operations*. Washington: Department of the Army, 1997.

USJFCOM, *Joint Forces Command Glossary,* vol. 2002: United States Joint Forces Command, 2002.

Webster's Ninth New Collegiate Dictionary, 9th ed. Springfield, MA: Werriam-Webster, Inc, 1984.

West, P.D., *Dynamic Risk Management of Network-Centric Systems*, Ann Arbor, MI; ProQuest, 2003.

Zeleny, M., *Multiple Criteria Decision Making*. New York: McGraw-Hill, 1982.

Appendix A: List of Symbols, Abbreviations and Acronyms

A	
AIAA	American Institute of Aeronautics and Astronautics
AUAV	Armed Unmanned Aerial Vehicle
AWE	Advanced Warfighting Experiment
C	
C4	Command, Control, Communications, Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CCRP	C4ISR Cooperative Research Program
CROP	Common Relevant Operating Picture
D	
DOD	Department of Defense
DRMM	Dynamic Risk Management Model
DSE	Department of Systems Engineering
DTIC	Defense Technical Information Center
E	
EBO	Effects-Based Operations
F	
FCS	Future Combat System
G	
GW	Global Weight
H	
HSI	Hypersonic Interceptor
HVAC	Heating, Ventilation, Air Conditioning
I	
IPT	Integrated Project Team
IT	Information Technology
J	
JIM	Joint Exercise Support System Intelligence Module
L	
LOS	Line of Sight
LW	Local Weight
M	
MAU	Multi-Attribute Utility
MBA	Master of Business Administration
METT-T	Mission, Enemy, Terrain, Troops, Time
MoD	Ministry of Defence
MOE	Measure of Effectiveness
N	
NCO	Network-Centric Operations
NCS	Network-Centric System
NCW	Network-Centric Warfare

O	
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OODA	Observe, Orient, Decide, Act
P	
P2P	Peer-to-Peer
Ph.D.	Doctor of Philosophy
S	
SA	Situation Awareness
SE	Systems Engineering
SEDD	Sensor and Electron Devices Directorate
SEDP	Systems Engineering Design Process
SOP	Standard Operating Procedure
U	
UA	Unit of Action
UE	Unit of Employment
UGV	Unattended Ground Vehicle
USMA	United States Military Academy
V	
VFT	Value-Focused Thinking

*This table is sorted alphabetically

Distribution List

NAME/AGENCY	ADDRESS	COPIES
Dr. Paul West	Department of Systems Engineering Mahan Hall West Point, NY 10996	2
Dr. Bobbie Foote	Department of Systems Engineering Mahan Hall West Point, NY 10996	2
Mr. Bob Walker	BAE Systems 310 Voyager Way Huntsville, AL 35806	1
Mr. Helmut Hass	SAIC 6725 Odyssey Drive Huntsville, AL 35806	1
Dean, USMA	Office of the Dean Building 600 West Point, NY 10996	1
Defense Technical Information Center (DTIC)	ATTN: DTIC-O Defense Technical Information Center 8725 John J. Kingman Rd, Suite 0944 Fort Belvoir, VA 22060-6218	1
Department Head-DSE	Department of Systems Engineering Mahan Hall West Point, NY 10996	1
ORCEN	Department of Systems Engineering Mahan Hall West Point, NY 10996	5
ORCEN Director	Department of Systems Engineering Mahan Hall West Point, NY 10996	1